Cisco Next Gen SD-WAN
Webinar 17 July 2018
Cisco SDWAN
Powered by Cisco Digital Network Architecture

Ronald Tan
Regional Sales Director
Enterprise Networking Sales
17 July 2018
What is SDWAN?

- Unified Threat Management?
- Link Diversity?
- Connectivity?
Second Wave of SDN Is Coming to the WAN

- Apps are moving to the cloud
  80/20 now becomes 20/80

- Mobile/IoT device proliferation
  Collaboration
  QoS

- Internet edge moving to the branch
  More requirements for security

Managing the network is getting more complex
Today’s WAN Challenges

- Insufficient Bandwidth
- Limited Application Awareness
- High Cost
- High Availability
- Complex Operations
- Limited Scale
- Fragmented Security
- No Cloud Apps Readiness

Is Your WAN Business Ready?
What Enterprise Customers Are Asking For?

Hybrid WAN
- Global, anywhere connectivity is the “new normal”
- MPLS
- Broadband
- 4G / LTE
- International Carriers

Cloud Adoption
- Highly available, optimal cloud connectivity options
- IaaS
- PaaS
- SaaS

Simplified Management
- Outsourced, managed network (CPE, DC, Campus)

Provide better security, Improve user experience, Shorten deployment times, Increase availability
Cisco SDWAN Architecture

- **On-premise or Cloud Managed**
- **Data Center**
- **Campus**
- **Branch**
- **Public Cloud**

- **Analytics and assurance**

- **Transport Independence**
- **Internet**
- ** LTE**

- **Network Services**
- **Unified Communications**
- **SD-WAN**
- **Application Hosting**
- **WAN Optimization**

- **End-point flexibility**
  - (Physical or Virtual)
  - **Public Cloud**
  - **Campus**
  - **Branch**
  - **Colocation**
  - **Data Center**

- **Integrated Security**
Spend less time troubleshooting WAN issues

- **End-to-end visibility**
  - 360-degree view across network
  - Historical view
  - Ability to follow the network path

- **Proactive and predictive insights**
  - Proactive to get ahead of the problem
  - Predictive to stay ahead
  - Assessment to see impact of changes

- **Guided remediation**
  - Today: Remediate with user input
  - Future: Automated remediation

Transform WAN Operations with actionable insights
Market Leading Routing + SD WAN

Leading Routing & SD-WAN Platforms

Cloud-managed & Feature-rich SD-WAN

DNA Center + SD-WAN

Vedge Router + vEdge SW
Cisco SD-WAN Platform Options

**Branch Services**
- **ISR 1000**
  - 200 Mbps
  - Next-gen connectivity
  - Performance flexibility
- **ISR 4000**
  - Up to 2 Gbps
  - Modular
  - Integrated service containers
  - Compute with UCS E
- **ASR 1000**
  - 2.5-200Gbps
  - High-performance service w/hardware assist
  - Hardware & software redundancy

**vEdge Appliances**
- **vEdge 100**
  - 100 Mbps
  - 4G LTE & Wireless
- **vEdge 1000**
  - Up to 1 Gbps
  - Fixed
- **vEdge 2000/5000**
  - 10 to 20 Gbps
  - Modular

**Virtualization**
- **ENCS 5100**
  - Up to 250Mbps
- **ENCS 5400**
  - 250Mbps – 2GB

**Simplified SDWAN Cloud**

**Public Cloud**
- Microsoft Azure
- Amazon Web Services
Cisco SD-WAN (Viptela)
Next-Gen Cisco SD-WAN Architecture

Shamil Fernando
Manager System Engineering (APAC & Japan)
shamilf@cisco.com
Cisco SD-WAN Solution Principals

- vManage
- vBond
- vAnalytics
- vSmart Controllers
- 3rd Party Automation
- APIs

Management/Orchestration Plane

Control Plane

Data Plane

Cloud
Data Center
Campus
Branch
CoLo

4G
MPLS
INET
Edge Routers
Cisco SD-WAN Solution Principals

- Separation Control and Data Plane
- DTLS/TLS is used to establish the control channel
- Control channel is established only with central controllers
- No scaling issues are with full mesh of control plane
- Control channel does not have to follow the data path
Cisco SD-WAN Solution
# Cisco SD-WAN Edge Devices

**18th July 2018**

## Branch Services
- **ISR 1000**
  - 200 Mbps
  - Next-gen connectivity
  - Performance flexibility
- **ISR 4000**
  - Up to 2 Gbps
  - Modular
  - Integrated service containers
  - Compute with UCS E
- **ASR 1000**
  - 2.5-200Gbps
  - High-performance service w/hardware assist
  - Hardware & software redundancy

## SD-WAN
- **vEdge 100**
  - 100 Mbps
  - 4G LTE & Wireless
- **vEdge 1000**
  - Up to 1 Gbps
  - Fixed
- **vEdge 2000**
  - 10 Gbps
  - Modular
- **vEdge 5000**
  - 20 Gbps
  - Modular

## Virtualization
- **ENCS 5100**
  - Up to 250Mbps
- **ENCS 5400**
  - 250Mbps – 2GB

## Private / Public Cloud
- [Microsoft Azure](#)
- [Amazon Web Services](#)
Zero-Trust Security Principles

- Strong authentication
  - PKI certificates, 2048bit keys
- Highly encrypted tunnels
  - DTLS/TLS AES256
  - White-list model
- Ubiquitous Deployment
  - Automatic NAT mitigation

Control Elements

X.509 Certificate
DTLS/TLS
Control Tunnel
Secure Bring-up With Approval

<table>
<thead>
<tr>
<th>Chassis Number</th>
<th>Certificate Serial</th>
<th>Hostname</th>
<th>IP Address</th>
<th>Validate</th>
</tr>
</thead>
<tbody>
<tr>
<td>9391da23-f0d1-4259..</td>
<td>0334D73E5EC036F87ABE..</td>
<td>DataCenter</td>
<td>1.1.1.5</td>
<td>invalid</td>
</tr>
<tr>
<td>4de0b85f-a2ae-42ec..</td>
<td>585A0084DEA8396DD77B..</td>
<td>RemoteSite</td>
<td>1.1.1.4</td>
<td>invalid</td>
</tr>
<tr>
<td>5f05358a-bef7-4e15..</td>
<td>248792F938E6E8BEE6FD..</td>
<td>AWS</td>
<td>1.1.1.6</td>
<td>invalid</td>
</tr>
</tbody>
</table>

- Per-device control on TPM identity trust
  - Single stage (Zero Touch Provisioning) – TPM identity is automatically trusted
  - Two stage (One Touch Provisioning) – TPM identity is not automatically trusted. Requires administrator validation.
- Staging Mode – TPM identity is automatically trusted for control, but not for data. Requires administrator validation.
End to End Security

- Each vEdge advertises its local IPsec encryption key

- Symmetric encryption IPsec AES256-GCM ESPv3 with HMAC SHA-1
- Traffic Encryption and Authentication Header
- Tunnel Liveliness Detection (BFD)
- Anti-Replay Protection
- Rekey **12 hours**
Application Quality of Experience

- Application Visibility
- SLA Based Policy
- Quality of Service (Queuing, Shaping and Marking)
- Application Aware Routing
- Path MTU Discovery
- Application Optimization (TCP Acceleration)
- Error Correction (FEC)
Application Visibility

Deep Packet Inspection
Over 3000+ application

- App Firewall
- Traffic prioritization
- Transport selection
Application Performances and AAR

By default, Cisco SDWAN performs flow-based load sharing across all transports available between the vEdge routers.

With Policies:
- Enforce SLA compliant path for applications of interest
- Other applications will follow active/active behavior across all paths

**App Aware Routing Policy**
App A path must have latency <150ms and loss <2%

**Path 1:** 10ms, 0% loss, 2ms jitter
**Path 2:** 200ms, 3% loss, 5ms jitter
**Path 3:** 140ms, 1% loss, 3ms jitter

**Optimal Throughput**

By default, Cisco SDWAN performs flow-based load sharing across all transports available between the vEdge routers. With Policies:
- Enforce SLA compliant path for applications of interest
- Other applications will follow active/active behavior across all paths

**App Aware Routing Policy**
App A path must have latency <150ms and loss <2%

**Path 1:** 10ms, 0% loss, 2ms jitter
**Path 2:** 200ms, 3% loss, 5ms jitter
**Path 3:** 140ms, 1% loss, 3ms jitter

**Optimal Throughput**
End to End Segmentation

- Isolated virtual private networks across any transport
- VPN mapping is based on physical vEdge Router interface, 802.1Q VLAN tag or a mix of both

Use Cases
- Security Zoning
- Compliance
- Guest WiFi
- Multi-Tenancy
- Extranet
Per-Segment Topologies

- **Full Mesh**
  - Unified Communications

- **Hub-and-Spoke**
  - Data Center Applications

- **Regional Hub**
  - Regional Internet/Services

**Optimal Application Experience**
Multiple Services Chaining

- vEdge routers with connected L4-L7 service make advertisement
  - Service route OMP address family
  - Services VPN labels
- Services are advertised in specific VPN
- Services can be L3 routed or L2 bridged
- Services can be singly or dually connected to the advertising vEdges
- Control or data policies are used to insert the service nodes into the matching traffic forwarding path
  - Match on 6-tuple of DPI signature
  - Applied on ingress/egress/service vEdge

* For data policy only. Control policy enforced on vSmart.
Secure Internet Access

- Can use one or more local DIA exits or backhaul traffic to the regional hub through the SD-WAN fabric and exit to Internet from there
  - Per-VPN behavior enforcement
- VPN default route for all traffic DIA or data policy for selective traffic DIA
- Network Address Translation (NAT) on the vEdge router only allows response traffic back
  - Any unsolicited Internet traffic will be blocked by IP table filters
- For performance based routing toward SaaS applications use Cloud onRamp
Cloud onRamp for SaaS

Internet DIA

- Remote Site
- ISP1
- ISP2
- SD-WAN Fabric
- Regional Hub
- Data Center

Loss/Latency

Application Quality Probing

Hybrid DIA

- Remote Site
- ISP1
- MPLS
- SD-WAN Fabric
- Regional Hub
- Data Center

Office 365
- Google
- Dropbox
- Salesforce

ISP1
ISP2
Data Center
A pair of vEdge routers is instantiated in Amazon VPC or Microsoft Azure VNET

- Gateway VPC/VNET

A pair of standard based IPSec tunnels is stretched from gateway VPC/VNET to each host VPCs/VNETs

- Connectivity redundancy

BGP is established across IPSec tunnels for route advertisement

- Bi-directional BGP/OMP redistribution on the gateway VPC/VNET vEdge routers

Entire process is automated through vManage workflow
Centralize Management & Monitoring

Centralize Configuration
- Security
- Template Configuration
- Policy
- Routing
- QoS, Marking
- ACL
- Application SLA
- ... .

Centralize Monitoring
- Devices
- Application
- Bandwidth usage
- Link Performances
- Alerts
Configuration Simplicity and ZTP

- Templates are attached to provisioned vEdge routers
- Variables are used for rapid bulk configuration rollout with unique per-device settings
- Local configuration changes are not allowed
  - Prevents configuration drift

<table>
<thead>
<tr>
<th>Status</th>
<th>Chassis Number</th>
<th>System IP</th>
<th>Hostname</th>
<th>Latitude</th>
<th>Longitude</th>
<th>System IP</th>
<th>Site ID</th>
<th>Bandwidth Upstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>4de0b85f-a2ae-42ec-8b45-3808285cd008</td>
<td>1.1.1.4</td>
<td>RemoteSite</td>
<td>37.33</td>
<td>-121.88</td>
<td>1.1.1.4</td>
<td>104</td>
<td>100</td>
</tr>
<tr>
<td>✔️</td>
<td>5f05358a-bef7-4e15-9ade-8fffd8f27ec93</td>
<td>1.1.1.6</td>
<td>AWS</td>
<td>45.52</td>
<td>-122.67</td>
<td>1.1.1.6</td>
<td>106</td>
<td>100</td>
</tr>
<tr>
<td>✔️</td>
<td>9391da23-f0d1-4259-88d9-e10ae714708c</td>
<td>1.1.1.5</td>
<td>DataCenter</td>
<td>40.71</td>
<td>-74.0</td>
<td>1.1.1.5</td>
<td>105</td>
<td>250</td>
</tr>
</tbody>
</table>
Configuration Simplicity and ZTP

Assumption:
- DHCP/Stic IP on Transport Side (WAN)
- DNS to resolve ztp.viptela.com*

* Factory default config

### Zero Touch Bringup Server
1. Query to ztp.viptela.com
2. Response with redirect to corporate orchestrator

### Control and Policy Elements
3. Initial control communication
4. Device configuration from Wmanage

### vEdge Router

- Authentication
- Push the configuration
- Enforce the version

Full Registration and Configuration
Self Healing Capabilities

1. Attach Template
   - vManage

2. Connectivity Lost
   - vEdge Router

3. Rollback
   - vEdge Router

Failed Upgrade

- Active Software: A
- Available Software: B
- Available Software: C
- Available Software: D

Activate

Rollback
Analytics Dashboard

Visibility
- Application Visibility
- Network Visibility
- Network Co-relation
- Cross-Customer Comparison

Forecast
- Application Usage Forecast
- Bandwidth Usage Forecast

What-If
- Branch Expansions
- Rolling out new applications
- Policy changes

Recommendation
Why Cisco SD-WAN
Trusted by Fortune 800 Enterprises

Viptela SEN: The Most-Deployed Enterprise Grade SD-WAN
Thousands of sites, every major industry, including:

- RETAIL
- HEALTHCARE
- FINANCIAL SERVICES
- ENERGY

Standards Compliant:
- HIPAA
- PCI

Most deployed and trusted by Fortune 500 enterprises
Winning 95% of competitive POCs
TOMORROW starts here.